UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/559,889	12/07/2005	Junbiao Zhang	PU030227	2851

24498 7590 06/18/2009

Thomson Licensing LLC
P.O. Box 5312
Two Independence Way
PRINCETON, NJ 08543-5312

EXAMINER	
NGUYEN, TRONG H	

ART UNIT	PAPER NUMBER
2436	

MAIL DATE	DELIVERY MODE
06/18/2009	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/559,889	ZHANG ET AL.	
	Examiner	Art Unit	
	TRONG NGUYEN	2436	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *27 May 2009*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1 and 3-14* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1 and 3-14* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. This action is in response to the communication filed on 05/27/2009. In response to the office action mailed on 02/27/2009, **claims 4 and 8-12** have been amended. Pending claims include **claims 1 and 3-14**.

The objection to claims **4 and 8-12** has been withdrawn due to applicants' amendments.

Examiner Notes

2. Examiner cites particular columns and line numbers in the references as applied to the claims below for the convenience of the applicant. Although the specified citations are representative of the teachings in the art and are applied to the specific limitations within the individual claim, other passages and figures may apply as well. It is respectfully requested that, in preparing responses, the applicant fully consider the references in entirety as potentially teaching all or part of the claimed invention, as well as the context of the passage as taught by the prior art or disclosed by the examiner.

Response to Arguments

3. Applicants' arguments filed 05/27/2009 have been fully considered but they are not persuasive.

Applicants argue that:

i. Lewis does not teach or suggest generating a new encryption key at the access point in claim 1 since the new encryption key is generated at the key distribution server 76 and provided to the access point (page 2 of REMARKS).

ii. Lewis does not disclose or suggest indicating a decryption failure in claim 1 since Lewis's access points simply pass or block messages that do not match the encryption key. Furthermore, the simple fact that packets get blocked cannot be construed as providing an indication (pages 2-3 of REMARKS).

iii. Lewis does not disclose or suggest maintaining an old encryption key and a new encryption key through a key rotation interval in claim 8 since Lewis discloses using the old key once and makes no further use of the old key after the new key has been sent. Moreover, this specific use of the old key takes place before the new key goes into effect (pages 3-4 of REMARKS).

In response to applicant's arguments:

i. The Examiner respectfully disagrees for the following reasons. The Examiner has interpreted "to generate" as "to bring into existence". Lewis discloses "Periodically, the access point 54 may be instructed to use a different or new ENCRYPT key" on col. 12, lines 42-44). Furthermore, note that the new ENCRYPT key originally did not exist in the access point. Thus, in order for the access point to use the new ENCRYPT key, this new ENCRYPT key must have existed in the access point. One way for the access point to bring this new ENCRYPT key into existence at the access point is by processing the message containing the new ENCRYPT key received from the key

distribution server 76 (e.g. receiving the message and extracting the new ENCRYPT key). Thus, Lewis does disclose "generating a new encryption key at the access point".

ii. The Examiner respectfully disagrees. The Examiner has interpreted “to indicate" as “to point out”. Lewis’s FIG. 7 discloses that messages received by an access point 54 from a mobile terminal are first evaluated to determine whether the messages have been encrypted by the current ENCRYPT key. If the received message is not encrypted using the current ENCRYPT key, the access point can: **a)** forward the message as originally received onto the system backbone 42 (col. 13, lines 22-24 and 34-36) **b)** forward the potentially unauthorized message to a predefined destination for further evaluation/unauthorized access detection (col. 13, lines 40-43 and col. 5, lines 63-65) **c)** block the received message (col. 13, lines 52-53). From option **b)** above, it can bee seen that by forwarding the potentially unauthorized message to a predefined destination for further evaluation/unauthorized access detection, the access point has pointed out or indicated to the predefined destination of the received message which was not encrypted by the current ENCRYPT key or a decryption failure. Therefore, Lewis does disclose indicating a decryption failure.

Moreover, Applicants assert that Jordan does not provide any indication of a decryption failure when a data frame fails to decrypt using the current encryption key. The Examiner respectfully disagrees. In Fig. 10 and col. 8, par. 0090, Jordan discloses the receiving device (which can be either the access gateway or the wireless device) after determining that the updated password key is incorrect (step 1315), it generates a

second message which is an error message containing information about the error or a request to resend the previous message using the based password key (or the password key that is prior to the most recent updated password key as mentioned in col. 8, par. 0093, lines 1-8) (step 1330) and transmits this error message to the other device (step 1340). In this manner, the device that receives the error message may revert back to the base password key (or the password key that is prior to the most recent updated password key) and resend the previous message using an encryption method using the based password key (or the password key that is prior to the most recent updated password key). Thus, Jordan does disclose indicating a decryption failure when a data frame fails to decrypt using the current encryption key.

iii. The Examiner respectfully disagrees for the following reasons. As explained in prior office action, Lewis does disclose “maintaining an old encryption key and a new encryption key". The question remains whether Lewis discloses "maintaining an old encryption key and a new encryption key **through a key rotation interval**." The Examiner has interpreted “a key rotation interval” as any period of time in which the access point (AP) posses both the new ENCRYPT key and the old ENCRYPT key for the process of key rotation. Lewis discloses "Periodically, the access point 54 may be instructed to use a different or new ENCRYPT key" (col. 12, lines 42-44) and the new ENCRYPT key is transmitted to the mobile terminal using the previous ENCRYPT key (col. 12, lines 44-46). The period of time from the point immediately after the generation of the new ENCRYPT key to the point immediately before the encryption of the new

ENCRYPT key using the previous ENCRYPT key at the AP can be reasonably viewed as the key rotation interval. In addition, the Examiner respectfully notes that the claimed limitation “maintaining an old encryption key and a new encryption key through a key rotation interval” as recited in claim 8 only requires maintaining (which is interpreted by the Examiner as “keeping in existence") an old encryption key and a new encryption key through a key rotation interval and does not specify how many times the old encryption key is being used or if the old encryption key is to be used before or after the new encryption key goes into effect.

Furthermore, Applicants assert that the feature of maintaining both keys through a certain interval is neither disclosed nor suggested in the cited art. The Examiner respectfully disagrees. The cited art, Jordan, discloses the claimed limitation of “maintaining an old encryption key and a new encryption key through a key rotation interval". Jordan discloses the messaging gateway 115 and the wireless device 135 continuously update their password keys (Fig. 8). However, upon a transmit or receiver error which results in their password keys being out of sync, the message gateway reverts back to a password key that is prior to the most recent updated password key (i.e. old password key) (Fig. 10 and col. 8, par. 0093, lines 1-8). Thus, Jordan discloses maintaining an old encryption key and a new encryption key. Using the same interpretation as mentioned above, the period of time from the point immediately after a new password key is generated to the point immediately before the next new password key is generated in the message gateway can be reasonably viewed as a key rotation interval. Through this key rotation interval, the access gateway maintains both the

current password key and the prior password key which allows it to decrypt messages encrypted using the current password key and decrypt messages encrypted using the prior password key in case the current password keys fall out of sync.

Therefore, **claims 1 and 8** are still unpatentable over the applied references and the same goes for their dependent claims. As a result, the rejection of **claims 1 and 3-14** is maintained.

Claim Rejections - 35 USC § 103

4. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

5. Claims **1**, **7-8** and **13** are rejected under 35 U.S.C. 103(a) as being unpatentable over Lewis US 6,526,506 (hereinafter "Lewis") in view of Jordan et al. US 2004/0081320 (hereinafter "Jordan").

Regarding claim **1**, Lewis discloses "**A key synchronization method for a wireless network comprising:**" as [the access point generates a new ENCRYPT key to be use as the current ENCRYPT key (Col. 12, lines 43-44), transmits the new ENCRYPT key to the mobile terminal (Col. 12, lines 44-46), and determines if the message received from the mobile terminal has been encrypted using the current ENCRYPT key (Col. 12, line 67-Col. 13, lines 1-2)] "**setting a current encryption key**

[ENCRYPT key (Col. 6, line 46)] **and an old encryption key** [previous ENCRYPT key (Col. 6, line 57)] **at an access point** [an access point 54 (Col. 6, line 55)] **in the wireless network**;" [wireless network (Col. 1, line 26)] "**generating a new encryption key at the access point**" as [Periodically, the access point may be instructed to use a different or new ENCRYPT key (Col. 12, lines 43-44)] "**resetting the current encryption key to equal the newly generated encryption key,**" as [since the access point is instructed to use a different or new ENCRYPT key (Col. 12, lines 43-44), it is obvious that the new ENCRYPT key now becomes the current encryption key] "**communicating the newly generated encryption key to the station in an encrypted form using the old encryption key**;" as [The access point communicates the new ENCRYPT key using the previous ENCRYPT key (Col. 12, lines 44-46)] "**indicating a decryption failure for a data frame received from the station when the encryption key used by the station does not match the current encryption key**" as [Fig. 7, access point determines if the message from received from the mobile terminal is encrypted with the current ENCRYPT key, if not, the access point follows appropriate actions described in steps 226-234]

Lewis does not specifically disclose "**resetting the old encryption key to equal an encryption key being used by a station in communication with the access point**" and "**wherein a data frame that failed to decrypt using the current encryption key is decrypted using the old encryption key**".

However, Jordan discloses a password key synchronization method wherein a message gateway reverts back to a password key that is prior to the most recent

updated password key (i.e. old password key) to decrypt a message received from a wireless device after unsuccessfully decrypting the message using the updated password key (i.e. current password key) (Figs. 10-11, Col. 8, Par. 0089, last 6 lines and Par. 0093, lines 1-8).

Jordan and Lewis are analogous art because they are in the same field of endeavor of secure data communication in a wireless network.

It would have been obvious to a person of ordinary skill in the art at the time of the invention to modify Lewis's invention by resetting the old encryption key to equal an encryption key being used by a station in communication with the access point and wherein a data frame that failed to decrypt using the current encryption key is decrypted using the old encryption key as described by Jordan for the purpose of resynchronizing password keys upon suffering a transmit or receive error (Jordan, Col. 8, Par. 0087, lines 3-6 and lines 13-15).

Regarding claim **7**, Lewis in view of Jordan discloses "**The method according to claim 1**, **wherein said step of setting is performed by the access point for each station in the wireless network**" as [see rejection to claim **1** above and Lewis's Fig. 1].

Regarding claim **8**, Lewis discloses "**A key synchronization system for a wireless network comprising**:" [the access point generates a new ENCRYPT key to be use as the current ENCRYPT key (Col. 12, lines 43-44), transmits the new ENCRYPT key to the mobile terminal (Col. 12, lines 44-46), and determines if the

message received from the mobile terminal has been encrypted using the current ENCRYPT key (Col. 12, line 67-Col. 13, lines 1-2)] "**at least one station in the wireless network**;" ["The wireless communication system 50 also includes one or more mobile terminals 66" (Fig. 1, Col. 4, lines 28-29)] "**and at least one access point in the wireless network** ["Connected to the system backbone 52 are several access points 54" (Fig. 1, Col. 4, lines 14-15)] **maintaining an old encryption key** [previous ENCRYPT key (Col. 6, line 57). *Note that the access point does maintain an old encryption key (i.e. previous ENCRYPT key) since the previous ENCRYPT key is used by the access point to provide the mobile terminal with a new ENCRYPT key (Col. 6, lines 55-57)*] **and a new encryption key through a key rotation interval for each of said at least one station** [Periodically, the access point may be instructed to use a different or new ENCRYPT key (Col. 12, lines 43-44) and the new ENCRYPT key is transmitted to the mobile terminal (Col. 12, lines 44-46)] **"said access point using said new encryption key when a first data frame correctly encrypted with said new encryption key is received from said at least one station"** [If the message is encrypted using the current ENCRYPT key as determined in step 222, the access point decrypts the message (Lewis, Fig. 7, Col. 13, lines 8-9). Furthermore, by disclosing when it is determined that the message received is not encrypted using the current ENCRYT key, the access point does not decrypt the message but proceeds to step 226 (Lewis, Fig. 7, Col. 13, lines 13-15, 34-35), Lewis also discloses the access point starts using the new ENCRYPT key when a first message correctly encrypted under the new ENCRYPT key is received from the mobile terminal]

Lewis does not specifically disclose "**and using said old encryption key when decryption of a data frame received from said at least one station fails due to mismatched keys**".

However, Jordan discloses a password key synchronization method wherein a message gateway reverts back to a password key that is prior to the most recent updated password key (i.e. old password key) to decrypt a message received from a wireless device after unsuccessfully decrypting the message using the updated password key (i.e. current password key) (Figs. 10-11, Col. 8, Par. 0089, last 6 lines and Par. 0093, lines 1-8).

Jordan and Lewis are analogous art because they are in the same field of endeavor of secure data communication in a wireless network.

It would have been obvious to a person of ordinary skill in the art at the time of the invention to modify Lewis's invention by "using said old encryption key when decryption of a data frame received from said at least one station fails due to mismatched keys" as described by Jordan for the purpose of resynchronizing password keys upon suffering a transmit or receive error (Jordan, Col. 8, Par. 0087, lines 3-6 and lines 13-15).

Regarding claim **13**, Lewis in view of Jordan discloses "**The method according to claim 1**, **wherein the new encryption key is generated at the access point upon expiration of a key refresh interval**" as [Periodically, the access point may be instructed to use a different or new ENCRYPT key (Lewis, Col. 12, lines 43-44)].

6. Claims **3**, **4**, **9** and **14** are rejected under 35 U.S.C. 103(a) as being unpatentable over Lewis in view of Jordan and further in view of Loc et al. US 7,293,289 (hereinafter "Loc").

Regarding claim **3**, Lewis in view of Jordan discloses "**The method according to claim 1**" and "**decrypting received data frames associated with said out-of-sync counter at the access point using the old encryption key**" as [see rejection to claim **1** above] but does not specifically disclose "**incrementing an out-of-sync counter in the access point when said decryption failure occurs due to the encryption key used by the station not matching the current encryption key"**.

However, Loc discloses a method for detecting a security breach in a network wherein "Each time a client 108 fails to successfully decrypt a packet, the encryption failure counter is incremented" (Fig. 5, Col. 6, lines 59-61).

Loc, Lewis, and Jordan are analogous art because they are in the same field of secure data communication in a wireless network.

It would have been obvious to a person of ordinary skill in the art at the time of the invention to modify the invention of Lewis in view of Jordan by incrementing an out-of-sync counter in the access point when said decryption failure occurs due to the encryption key used by the station not matching the current encryption key as described by Loc in order to detect a security breach in a network (Loc, Col. 1, lines 22-23).

Regarding claim **4**, Lewis in view of Jordan discloses "**The method according to claim 1, further comprising: decrypting, using the new encryption key the received data frame from the station when the access point determines the station sending the received packet is using the new encryption key, said access point starting to use the new encryption key when a first data frame correctly encrypted with the new encryption key is received from the station;**" as [If the message is encrypted using the current ENCRYPT key as determined in step 222, the access point 54 decrypts the message (Lewis, Fig. 7, Col. 13, lines 8-9). Furthermore, by disclosing when it is determined that the message received is not encrypted using the current ENCRYT key, the access point does not decrypt the message but proceeds to step 226 (Lewis, Fig. 7, Col. 13, lines 13-15, 34-35), Lewis also makes it obvious that the access point starts using the new ENCRYPT key when a first message is correctly encrypted under the new ENCRYPT key by the mobile terminal. Moreover, Jordan also discloses this limitation on Figs. 10-11, Col. 8, Pars. 0088-0089] "**re-setting the old encryption key to equal the current encryption key when decryption is successful;** as [Jordan discloses the message gateway receives an encrypted first message (at step 1305 of Fig. 10) and decrypts it with an updated password key (step 1310 of Fig. 10) and if the updated password key is correct, then the decrypted message is displayed (step 1320 of Fig. 10). If the updated password key is incorrect, then the message gateway reverts back to a password key that is prior to the most recent updated password key (i.e. old password key) (step 1325 of Fig. 10) or in other words the current password key is the old password key. Then the process proceeds

through steps 1330-1340 and back to step 1305. Thus, it is obvious that the old password key is reset to the current password key once the updated password key is correct or in other words the updated password key becomes the current password key and the current password key becomes the old password key] but does not specifically disclose **"and re-setting an out-of-sync counter to zero upon successful decryption**".

However, Loc discloses a method for detecting a security breach in a network wherein "Each time client 108 successfully decrypts a packet, the encryption failure counter is reset to zero" (Loc, Col. 6, lines 57-69).

Loc, Lewis, and Jordan are analogous art because they are in the same field of secure data communication in a wireless network.

It would have been obvious to a person of ordinary skill in the art at the time of the invention to modify the invention of Lewis in view of Jordan by re-setting an out-of-sync counter to zero upon successful decryption as described by Loc in order to detect a security breach in a network (Loc, Col. 1, lines 22-23).

Regarding claim **9**, Lewis in view of Jordan discloses "**The key synchronization system according to claim 8**" but does not specifically disclose "**wherein said at least one access point further maintains an out-of-sync counter to track the number of packets where decryption fails due to mismatched keys**".

However, Loc discloses a method for detecting a security breach in a network wherein "Each time client 108 fails to successfully decrypt a packet, the encryption failure counter is incremented" (Fig. 5, Col. 6, lines 59-61).

Loc, Jordan and Lewis are analogous art because they are in the same field of secure data communication in a wireless network.

It would have been obvious to a person of ordinary skill in the art at the time of the invention to modify the invention of Lewis in view of Jordan by including an encryption failure counter at the access point which keeps track of the number of packets that were not successfully decrypted due to mismatched keys as described by Loc in order to detect a security breach in a network (Loc, Col. 1, lines 22-23).

Regarding claim **14**, Lewis in view of Jordan and further in view of Loc discloses "**The method according to claim 3, wherein said out-of-sync counter comprises a predetermined threshold that if exceeded causes communication to terminate between the access point and a source of the data frames causing the threshold of said out-of-sync counter to be exceeded**" as ["When the encryption failure counter reaches a predetermined threshold n (that is, when n consecutive failures have occurred) (step 512), client 108 sends an alert packet to access point" (Loc, Col. 6, lines 61-65). Furthermore, upon receiving the alert of a security breach, the access point "responds by immediately removing the MAC address of client 108 from its list of authorized clients, by ceasing to send any packets to the MAC address of client 108,

and by discarding all packets that are received from the MAC address of client 108" (Loc, Col. 6, lines 5-9)].

7. Claims **5-6 and 10-12** are rejected under 35 U.S.C. 103(a) as being unpatentable over Lewis in view of Jordan and further in view of Kelem et al. US 6,118,869 (hereinafter "Kelem").

Regarding claim **5**, Lewis in view of Jordan discloses "**The method according to claim 1"** but does not specifically disclose **"further comprising setting the old encryption key equal to a null value, said null value representing a no encryption mode**".

However, Kelem discloses if decryption is not desired, a decryption key value of 0 is chosen (Col. 4, lines 18-20). By disclosing setting a decryption key to a null value or 0 when no decryption is desired, Kelem also makes it obvious to set an encryption key to a null value when no encryption is desired.

Kelem, Lewis, and Jordan are analogous art because they are in the same field of endeavor of encryption and/or decryption key protection.

It would have been obvious to a person of ordinary skill in the art at the time of the invention to modify the invention of Lewis in view of Jordan by setting the old key equal to a null value, said null value representing a no encryption mode as taught by Kelem in order to modify the key thereby providing a high level of security (Kelem, Col. 2, lines 10-14).

Regarding claim **6**, Lewis in view of Jordan discloses "**The method according to claim 1,**" but does not specifically disclose "**further comprising setting the current encryption key and the old encryption key to a null value, said null value representing a no encryption mode**".

However, Kelem discloses if decryption is not desired, a decryption key value of 0 is chosen (Col. 4, lines 18-20). By disclosing setting a decryption key to a null value or 0 when no decryption is desired, Kelem also makes it obvious to set an encryption key to a null value when no encryption is desired.

Kelem, Lewis, and Jordan are analogous art because they are in the same field of endeavor of encryption and/or decryption key protection.

It would have been obvious to a person of ordinary skill in the art at the time of the invention to modify the invention of Lewis in view of Jordan by setting the current encryption key and the old encryption key to a null value, said null value representing a no encryption mode as taught by Kelem in order to modify the keys to provide a high level of security (Kelem, Col. 2, lines 10-14).

Regarding claim **10**, Lewis in view of Jordan discloses "**The key synchronization system according to claim 8**," but does not specifically disclose "**wherein said at least one access point is capable of setting the old encryption key to a null value, said null value representing a no encryption mode**".

However, Kelem discloses if decryption is not desired, a decryption key value of 0 is chosen (Col. 4, lines 18-20). By disclosing setting a decryption key to a null value

or 0 when no decryption is desired, Kelem also makes it obvious to set an encryption key to a null value when no encryption is desired.

Kelem, Jordan and Lewis are analogous art because they are in the same field of endeavor of encryption and/or decryption key protection.

It would have been obvious to a person of ordinary skill in the art at the time of the invention to modify the invention of Lewis in view of Jordan by setting the old encryption key at the access point to a null value which represents a no encryption mode as taught by Kelem in order to modify the key thereby providing a high level of security (Kelem, Col. 2, lines 10-14).

Regarding claim **11**, Lewis in view of Jordan discloses "**The key synchronization system according to claim 8**," but does not specifically disclose "**wherein said at least one access point is capable of setting the new encryption key to a null value, said null value representing a no encryption mode**".

However, Kelem discloses if decryption is not desired, a decryption key value of 0 is chosen (Col. 4, lines 18-20). By disclosing setting a decryption key to a null value or 0 when no decryption is desired, Kelem also makes it obvious to set an encryption key to a null value when no encryption is desired.

Kelem, Jordan and Lewis are analogous art because they are in the same field of endeavor of encryption and/or decryption key protection.

It would have been obvious to a person of ordinary skill in the art at the time of the invention to modify the invention of Lewis in view of Jordan by setting the new

encryption key at the access point to a null value which represents a no encryption mode as taught by Kelem in order to modify the key thereby providing a high level of security (Kelem, Col. 2, lines 10-14).

Regarding claim **12**, Lewis in view of Jordan discloses "**The key synchronization system according to claim 8**," but does not specifically disclose "**wherein said at least one access point initially sets the old encryption key to a null value**".

However, Kelem discloses if decryption is not desired, a decryption key value of 0 is chosen (Col. 4, lines 18-20). By disclosing setting a decryption key to a null value or 0 when no decryption is desired, Kelem also makes it obvious to set an encryption key to a null value when no encryption is desired.

Kelem, Jordan and Lewis are analogous art because they are in the same field of endeavor of encryption and/or decryption key protection.

It would have been obvious to a person of ordinary skill in the art at the time of the invention to modify the invention of Lewis in view of Jordan by setting the old encryption key at the access point initially to a null value which represents a no encryption mode as taught by Kelem in order to modify the key thereby providing a high level of security (Kelem, Col. 2, lines 10-14).

Conclusion

THIS ACTION IS MADE FINAL. See MPEP 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to TRONG NGUYEN whose telephone number is (571)270-7312. The examiner can normally be reached on Monday through Thursday 7:30 AM - 5:00 PM EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, NASSER MOAZZAMI can be reached on (571)272-4195. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/T. N/
Examiner

/David García Cervetti/

Primary Examiner, Art Unit 2436